Notice of Allowability	Application No.	Applicant(s)	
	09/909,709	KUEHR-MCLAREN ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *07 February 2005*.

2. ☒ The allowed claim(s) is/are *1-46*.

3. ☒ The drawings filed on *20 July 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1-46 are pending.

2. Arguments filed 02/07/2005 have been received and considered.

Allowable Subject Matter

3. Applicant's argument that the modified Gennaro, CSU, and Wagner system fails to disclose would not transmit packets with a group MAC without including an associated MAC with ones of the packets is persuasive. Therefore the following is an examiner's statement of reasons for allowance: the claimed limitations of the transmission and reception of packets sent over a SSL-based protocol connection along with the generated group MAC, wherein ones of the plurality of communication packets do not include an associated packet MAC would not have been obvious at the time of the invention to one skilled in the art. Using the group MAC in an SSL-based protocol, as above, would not have been obvious since SSL-based protocols attach a MAC to each packet sent. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

4. Applicant's arguments: the packets of the modified Gennaro, CSU, and Wagner system do not comply with the SSL packets of Applicant's invention; Gennaro is directed to digital signatures not MACs; Gennaro is related to message streams; Wagner teaches away from modifying the SSL packet MAC construction; Gennaro fails to disclose the "record count"; and the modified Gennaro, CSU, and Wagner system fails to disclose would not transmit packets with a group MAC without including an associated MAC with ones of the packets are not persuasive.

The packets of the modified Gennaro, CSU and Wagner system comply with the SSL packets of Applicant's invention because when using the SSL based communication of Wagner the data being transmitted are SSL packets as described in Applicant's specification on page 12 lines 22-24 that all SSL-based protocols include a MAC for each packet.

Gennaro is directed to the use of digital signatures, but Applicant is referred to the bottom of page 3 where Gennaro discloses, "if the receiver were only interested in establishing the identity of the sender, a solution based on MAC would suffice." This shows the use of MACs could be used in the system.

Gennaro discloses breaking the streams into blocks (see page 3 paragraph 3) and the modification of CSU would be for those blocks to be packets.

Wagner teaches modification of SSL, where stated that "SSL 2.0 uses a weak MAC construction" teaches that SSL 2.0 needs a better MAC construction and therefore should be modified.

Gennaro teaches the "record count" as disclosed at page 3, paragraph 3, where the table has a table of contents and that table of contents would show the hash of each block.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Wong et al, Golle et al, Miner et al, Park et al, Perrig et al, and CMU disclose methods for using group MACs. Metzger et al discloses IP-MAC, Hoffman and Dierks et al disclose the use of TSL.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be

reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER